19-1204

United States Court of Appeals for the Fourth Circuit

FRANK HEINDEL; PHIL P. LEVENTIS,
Plaintiff-Appellants,

v.

MARCI ANDINO, Executive Director of the South Carolina State Election Commission, in her official capacity; JOHN WELLS, Chair of the South Carolina State Election Commission, in his official capacity; CLIFFORD J. ELDER, AMANDA LOVEDAY, SCOTT MOSELY, Members of the South Carolina State Election Commission, in their official capacity,
Defendant-Appellees

Appeal from the United States District Court for the District of South Carolina in No. 3:18-cv-01887-JMC, Judge J. Michelle Childs

BRIEF OF THE NATIONAL ELECTION DEFENSE COALITION AND ELECTION SECURITY EXPERTS* AS AMICI CURIAE IN SUPPORT OF PLAINTIFF-APPELLANTS AND REVERSAL

John D. Graubert
Philip S. May
Counsel of Record
Megan O'Neill
Adam G. Crews
Jessica Jensen
COVINGTON & BURLING LLP
850 Tenth Street, NW
Washington, DC 20001-4956
(202) 662-6000

Ronald Fein
John Bonifaz
FREE SPEECH FOR PEOPLE
1340 Centre St. #209
Newton, MA 02459
(617) 244-0234

Counsel for Amici Curiae

April 15, 2019

*A full list of *amici* appears in the brief's Statement of Interest.

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 19-1204 Caption: Frank Heindel v. Marci Andino

Pursuant to FRAP 26.1 and Local Rule 26.1,

the National Election Defense Coalition (NEDC)
(name of party/amicus)

who is amicus, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☑ YES ☐ NO
If yes, identify all parent corporations, including all generations of parent corporations:
Psephos, Inc.

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☐ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: s/ Philip S. May Date: 4/15/2019

Counsel for: Amicus NEDC

CERTIFICATE OF SERVICE

****

I certify that on April 15, 2019 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

Protect Democracy Project, Inc.
125 Walnut Street, Suite 202
Watertown, MA 02472

510 Meadowmont Village Circle, No. 328
Chapel Hill, NC 27517

2020 Pennsylvania Ave, NW, No. 163
Washington, DC 20006

Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036

Office of the Attorney General of South Carolina
P.O. Box 11549
Columbia, SC 29211

s/ Philip S. May
(signature)

04/15/2019
(date)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

STATEMENT OF INTEREST

All parties have consented to the filing of this brief. No party or counsel for a party authored this brief in whole or in part. No party, counsel for a party, or person other than *amici curiae* and their counsel made any monetary contribution intended to fund the preparation or submission of this brief.

Amici curiae are the National Election Defense Coalition (NEDC) and election security experts. The NEDC is a national network of recognized experts in cybersecurity and elections administration, bipartisan policymakers, and concerned citizens. The NEDC works to build a bipartisan consensus on the need for reform, while building a comprehensive, cost-effective plan to secure the vote in coming elections.

Amici are also the following individuals with expertise in the security of electronic voting systems:[1]

Duncan A. Buell, Professor, Department of Computer Science and Engineering and NCR Chair of Computer Science and Engineering, University of South Carolina.

[1] Institutional affiliations are provided for identification purposes only and do not constitute or reflect institutional endorsement.

Richard DeMillo, Professor, Charlotte B. and Roger C. Warren Chair of Computing, and Director of the Center for 21st Century Universities (C21U), Georgia Institute of Technology.

Douglas W. Jones, Associate Professor, Department of Computer Science, University of Iowa.

Joseph R. Kiniry, Principal Scientist, Galois and Principled CEO and Chief Scientist, Free & Fair.

Peter G. Neumann, Chief Scientist, SRI International Computer Science Lab.

Bruce Schneier, Adjunct Lecturer in Public Policy, Harvard Kennedy School, and Fellow at the Berkman Klein Center for Internet & Society, Harvard University.

Philip B. Stark, Associate Dean, Division of Mathematical and Physical Sciences, and Professor of Statistics, University of California.

Poorvi L. Vora, Professor of Computer Science, The George Washington University.

Dan S. Wallach, Professor of Computer Science and Rice Scholar, Baker Institute for Public Policy, Rice University.

SUMMARY OF ARGUMENT

South Carolina's electronic voting system—the ES&S iVotronic Direct Recording Electronic (DRE) system—imparts real and imminent injury on the federally protected right to vote. The iVotronic system arbitrarily dilutes voting power by double- and under-counting certain votes, thereby empowering certain voters at the expense of others. It also assigns votes to incorrect candidates and lacks adequate means to audit reported results, all of which increase the system's arbitrary treatment of ballots. In addition, known defects in the voting system make it uniquely susceptible to undetectable foreign and domestic interference by attackers. South Carolina's refusal to guard against these attacks is tantamount to turning a blind eye to ballot box tampering. For all of these reasons, this system interferes with the ability of South Carolina residents—including Plaintiffs—to exercise their rights to vote. The Court should reverse the district court's dismissal of Plaintiffs' Complaint.

ARGUMENT

Judicial protection of the right to vote has a storied history in the Anglo-American legal tradition. Over 300 years ago, the courts in England recognized that the "right of voting is a right in the plaintiff by the common law, and consequently he shall maintain an action for the obstruction of it." *Ashby v. White*, 2 Ld. Raym. 938, 954 (K.B. 1702). And in this country, the federal courts have for

over 130 years regarded "the political franchise of voting" as "fundamental" and "preservative of all rights." *Yick Wo v. Hopkins*, 118 U.S. 356, 370 (1886). In light of that foundational status, the Supreme Court has directed that "any alleged infringement of the right of citizens to vote must be carefully and meticulously scrutinized." *Reynolds v. Sims*, 377 U.S. 533, 562 (1964). Without recourse to judicial protection of the right to vote, we might still distort legislative districts, *Wesberry v. Sanders*, 376 U.S. 1, 8 (1964), disenfranchise the poor, *Harper v. Va. State Bd. of Elections*, 383 U.S. 663, 666 (1966), or overburden ballot access, *Williams v. Rhodes*, 393 U.S. 23, 31 (1968).

Despite this long history of robust constitutional standards, many states—South Carolina among them—still use voting systems rife with errors and vulnerabilities. Some votes go uncounted, while others are counted twice. Systems that are entirely paperless allow arbitrary errors to go unnoticed and uncorrected. And foreign state actors and domestic threats lie in wait to manipulate the ballot box, while states have no way to prevent such interference.

The Plaintiffs in this lawsuit chose to stand up to these problems and to vindicate their right to vote by demanding that South Carolina provide a voting system without the real and immediate vulnerabilities currently known to exist. At present, South Carolina relies on unauditable paperless iVotronic direct-recording electronic (DRE) machines, which have well-documented errors and

vulnerabilities—including double-counting votes, under-counting votes, and assigning votes to the wrong candidates, all without an effective mechanism to audit results. Those deficiencies cause real harm to voters like Plaintiffs who stand to have their votes undervalued and their electoral preferences frustrated.

Plaintiffs never had the chance to press their claim on the merits. Instead, the district court concluded that they could not even bring their case because their injuries were merely speculative. That decision misunderstood the nature of Plaintiffs' injuries and underestimated what election and national security experts recognize as the serious flaws in voting systems like South Carolina's. As courts are already beginning to recognize, "[a]dvanced [and] persistent threats in this data-driven world and ordinary hacking[s] are unfortunately here to stay." *Curling v. Kemp*, 334 F. Supp. 3d 1303, 1328 (N.D. Ga. 2018). The best way to fight back against these threats is to accept "the research-based findings of national cybersecurity engineers and experts in the field of elections." *See id*. Those expert findings confirm that the problems with South Carolina's paperless iVotronic DRE machines are real, well-known, and likely to recur.

I. Plaintiffs' Injuries Are Real, Certain, and Imminent.

The right to vote is about more than just access to the polls. Indeed, the Supreme Court has identified at least three ways in which a state can impair the right to vote: States cannot arbitrarily dilute votes, *see Baker v. Carr*, 369 U.S.

186, 208 (1962); *see also Reynolds*, 377 U.S. at 558 (the Constitution's "conception of political equality" requires that votes be afforded equal weight (quoting *Gray v. Sanders*, 372 U.S. 368, 381 (1963))); states cannot "refus[e] to count votes from arbitrarily selected precincts," *Baker*, 369 U.S. at 208; and state action cannot result in "a stuffing of the ballot box," *id*.

An abridgement of any of these guarantees "present[s] a justiciable controversy subject to adjudication by federal courts." *See Reynolds*, 377 U.S. at 556. And any voter may bring a lawsuit "where large numbers of voters suffer interference with voting rights conferred by law." *FEC v. Akins*, 524 U.S. 11, 24 (1998); *see also Gray*, 372 U.S. at 375 (1963) ("any person whose right to vote is impaired . . . has standing to sue" (internal citations omitted)); *Mich. State A. Philip Randolph Inst. v. Johnson*, 209 F. Supp. 3d 935, 944 (E.D. Mich. 2016) ("[V]oters can have standing based on an increased risk that their voting rights will be infringed."). "An allegation of future injury may suffice if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (internal quotation marks omitted). Indeed, courts have described the ability to maintain a suit as "broad" where the challenge is to an electoral system that advantages some voters over others. *See Citizens in Charge v. Husted*, 2011 WL 3652701, at *3 (S.D. Ohio Aug. 19, 2011); *see also Black v. McGuffage*, 209 F. Supp. 2d 889, 895 (N.D.

Ill. 2002) (finding standing based on a "probabilistic" injury when the harm asserted was "not the State's failure to count any one person's vote, but the higher probability of that vote not being counted as a result of the voting systems used").

The Plaintiffs' claims in this case implicate each of the core voting rights described in *Baker*.

First, Plaintiffs are challenging a voting system that has already diluted their votes. The errors in South Carolina's system include double-counting some votes, while not counting others—both of which affect a dilution of voting power.

Second, South Carolina's voting system has already arbitrarily resulted in undercounted votes. It also arbitrarily assigns votes to the wrong candidates. And these arbitrary errors go undetected and uncorrected because South Carolina's entirely paperless system cannot be audited.

Third, with the growing threat of malicious election interference from at home and abroad, South Carolina has chosen to use a voting system that is known to be particularly susceptible to sophisticated, high-tech ballot box tampering.

South Carolina's flawed voting system will injure Plaintiffs again. By their very nature, systems are organized around a defined set of principles and procedures. If those principles and procedures are faulty—as South Carolina's are, and are alleged to be—then there is no reason to expect that past failures will not recur. But even more fundamentally than that, "[a] wound or reasonably

threatened wound to the integrity of a state's election system carries grave consequences beyond the results in any specific election, as it pierces citizens' confidence in the electoral system and the value of voting." *Curling*, 334 F. Supp. 3d at 1328.

A. South Carolina's Voting System Dilutes Voting Power.

The law is settled that "the right of suffrage can be denied by a debasement or dilution of the weight of a citizen's vote just as effectively as by wholly prohibiting the free exercise of the franchise." *Reynolds*, 377 U.S. at 555; *Locklear v. N.C. State Bd. of Elections*, 514 F.2d 1152, 1154 (4th Cir. 1975); *see also Curling*, 334 F. Supp. 3d at 1316 (voters' allegation "that their votes would likely be improperly counted based on the use of certain voting technology" was sufficient to maintain a lawsuit). South Carolina's voting system causes that injury: It arbitrarily allows some voters' votes to count twice, while others are unable to vote at all.

A recent study has uncovered that in the 2018 primary election in Marlboro County, South Carolina, "there were apparently 148 voters who had the distinct privilege of voting twice." Duncan Buell & Gregory Gay, *Is Technology the Answer? Software Quality Issues in Electronic Voting Systems*, J. of Sys. & Software (forthcoming), at 25 (hereinafter Buell & Gay, *Is Technology the Answer?*), *available at* https://cse.sc.edu/~buell/Public_Data/2019_

VotingMachines.pdf. Due to a system failure, 148 votes were reported twice in the final tallies, in effect giving the voter two ballots instead of just one. The error was not caught at either the county or state level—"the totals as reported are simply wrong." *Id*.

Over-counting errors of this sort are not new in South Carolina. As early as 2005, South Carolina's electronic voting system has overstated vote totals. *See* Lawrence Norden, *Voting System Failures: A Database Solution*, Appendix B, at 87 (2010), *available at* https://www.brennancenter.org/sites/default/files/legacy/Democracy/Voting_Machine_Failures_Online.pdf (hereinafter, Norden, *Voting System Failures*). In one local election, the electronic voting machines reported 3,208 votes when in fact only 768 had been cast. *Id*. "Election officials suspected that the error occurred because machine cartridges were incorrectly programmed to record some votes more than once." *Id*.

The double-counting error is no different from the voting rights injuries that courts routinely redress. By arbitrarily allowing some voters to vote twice, South Carolina's voting system has diluted the voting power of every other South Carolina voter—Plaintiffs included.

At the other end of the spectrum, the same study that uncovered double-counting identified a fault "known to cause votes not to be counted." Buell & Gay, *Is Technology the Answer?*, at 26. In 2012, this failure left 129 votes in Richland

County, South Carolina, uncounted. Worse yet, "this fault is difficult to detect," and indeed the specific under-counting error "was detected entirely by chance." *Id*. The investigators concluded that that the failure has "probably" gone undetected in other instances as well. *Id*. And without additional investigation, there is no way to know whether the fault still persists. *See id*. at 27.

It is no answer to say that the Plaintiffs may or may not be able to prove that their particular votes have been, or will be, undercounted. The failure to count *any* number of votes affects a debasement or dilution of voting power for others. When compared with voters in districts affected by under-counting, voters in any district where the error did *not* occur will have a harder time electing their chosen representative because they must compete with more total votes in the voting pool.

These errors—over- and under-counting—will recur in future elections because they are systematic errors. As two experts explained, there is an "inherent problem" in trying to detect software errors in voting systems: "there is no way to determine [the] ground truth of the results and virtually no way to test the software at scale[.]" Buell & Gay, *Is Technology the Answer?*, at 39. The software errors in South Carolina's voting system include those that have survived revisions and upgrades and those that cannot be detected with election data alone, because the error is an incorrect declaration that there is no data. *Id*. Moreover, the South Carolina system "does not provide sufficient failsafe mechanisms to decrease the

likelihood of simple mistakes." *Id.* Taken together, these vulnerabilities led the election security experts to the same intuitive conclusion that the law requires: "[E]ach software fault arguably causes *great damage* to the users and environment of the system by falsely amplifying, misrepresenting, or disenfranchising their vote." *Id.* at 40 (emphasis in original).

B. South Carolina's Voting System Arbitrarily Frustrates Voters' Abilities To Elect Their Preferred Candidate.

Apart from diluting voting power, South Carolina's error-prone voting system arbitrarily frustrates voter choices. "The Constitution protects the right of qualified citizens . . . to have their votes counted as cast." *Hendon v. N.C. State Bd. of Elections*, 710 F.2d 177, 180 (4th Cir. 1983). But South Carolina's system under-reports votes or arbitrarily assigns them to the wrong candidates.

As already noted, South Carolina's voting system suffers from systematic issues that result in the deletion of votes. *See* Part I-A, *supra*. Those errors have occurred in the past and are likely to occur again. *See id.*

Apart from undercounting, however, South Carolina's paperless iVotronic DRE terminals have well-documented issues with assigning votes to the wrong candidates. In Richland County, where votes were under-counted in 2012, the 2018 election was more of the same. There were "several reports of malfunctioning voting machines" in which voters "report[ed] the final voting submission page did not reflect their intended vote, saying their vote 'flipped.'"

Shelby Heary, "Richland County says review your ballots after voting issues reported," *WLTX19* (Nov. 6, 2018), *available at* https://www.wltx.com/article/news/politics/elections/richland-county-says-review-your-ballots-after-voting-issues-reported/101-611652645. And Richland County is not alone in facing voting machine failures of this sort. York County voters faced the same issues, with voting machines flipping their votes from their candidate of choice to an alternative candidate. Hannah Smoot, "'Check your ballot:' York County election machine snafu reported that changed vote," *The Herald* (Nov. 6, 2018), https://www.heraldonline.com/news/local/article221199050.html; *see also* Norden, *Voting System Failures*, Appendix B, at 86–87.

These errors are likely to recur, which South Carolina's local election officials admit. The Richland County Elections Director, Rokey Suleman, reported that the problems in his jurisdiction "were caused by a calibration issue with the voting machines" and "if the touchscreen calibration was off, it could make an unintended selection." Heary, *supra*. Suleman told reporters that "we're going to start seeing more mechanical issues, more hardware issues, some more software issues. That's why it's really important that we try to transition to new voting equipment as quickly as possible." *Id.*

And that is not the end of the vulnerabilities. Researchers have identified another problematic aspect of the iVotronic DRE machines in South Carolina that

could hinder voters' abilities to cast votes for their preferred candidates. The software permits individual voting terminals to have a list of contests different from the county's central computer, and it adds votes from those terminals "based on cell location in a spreadsheet, not based on keys for the contest names." *See* Buell & Gay, *Is Technology the Answer?*, at 28–29. Where the lists differ—even slightly—between the terminals and the central computer, this problem causes voter selections of particular candidates to become misaligned and ultimately recorded incorrectly. The researchers observed anomalies that were likely caused by this error in both the 2010 and 2018 elections in South Carolina. *See id.*

The deficiencies in South Carolina's system are compounded by the absence of an audit trail. "Election audits are critical to ensuring the integrity of election outcomes and for raising voter confidence." *See* The National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* 93 (2018), *available at* https://www.nap.edu/read/25120/chapter/1 (hereinafter NASEM, *Securing the Vote*). The reason is straightforward: Audits "demonstrate the validity of an election outcome and provide an indication of errors in ballot tabulation." *Id.* at 93–94. In that connection, a paper ballot trail is "a simple form of . . . evidence" that can "provide assurance that the reported outcome indeed is the result of a correct tabulation of cast ballots." *Id.* at 94. In fact, the National Academies of Sciences, Engineering, and Medicine recently

concluded that a paper audit trail "is generally preferred over electronic evidence," because electronic evidence "can be altered by compromised or faulty hardware or software." *Id*. In short, a statistically robust and paper-based audit is a fundamental control against the risk of arbitrary electronic voting errors of the sort that are well-known in South Carolina.[2]

But South Carolina's paperless DREs have no paper voter-marked ballots that can be audited to determine whether the electronic voting machines performed as intended. Instead, the *only* way to audit South Carolina's DREs is by using data, but if the data itself is corrupted—such as from a software error—then the audit will not shed light on the underlying problems. *Cf.* Buell & Gay, *Is Technology the Answer?*, at 39 (observing that an "inherent problem" with an analysis based only on data is that "there is no way to determine ground truth"). Without a paper ballot audit trail, errors in electronic voting systems like South Carolina's are likely to go undetected and uncorrected, thereby burdening the right to vote in election after election.

Experts have already reached this conclusion. When the U.S. Election Assistance Commission tasked the National Institute of Standards and Technology

[2] Importantly, a paper-based audit trail does *not* mean that states must use a ballot that voters mark by hand. A DRE machine could, for instance, generate a paper printout reflecting the votes cast. This would leverage the benefits of technology without sacrificing a voter-marked audit trail. *See* NIST, *Report of the Auditability Working Group* 28 (Jan. 14, 2011), *available at* https://www.eac.gov/assets/1/28/AuditabilityReport_final_January_2011.pdf.

("NIST") with developing ways to audit DRE-based systems without a paper ballot, NIST could not identify a viable option. Instead, NIST concluded that "[t]he main shortcoming of paperless DREs is in transparency and auditability: they *do not provide the capacity* for observers, or election officials, to confirm for themselves that the voting equipment worked properly in any particular election." NIST, *Report of the Auditability Working Group* 28 (Jan. 14, 2011), *available at* https://www.eac.gov/assets/1/28/AuditabilityReport_final_January_2011.pdf (emphasis added). "As a result, errors and failures of the equipment may go undetected, which can lead to significant undetected errors in the vote tally." *Id*.

NIST is not alone in its conclusions about the problems with paperless voting systems. As the nonpartisan experts at Harvard's Defending Digital Democracy Project explained, "[t]o protect against cyber-attacks or technology failures jeopardizing an election, it is essential to have a voter-verified auditable paper record to allow votes to be cross-checked against election results." Defending Digital Democracy Project, Belfer Center for Science and International Affairs, *The State and Local Election Cybersecurity Playbook* 15 (Feb. 2018), *available at* https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf. "Any security vulnerability in th[e voting machine's] hardware or software, or any ability for an attacker to alter (or reload new and maliciously behaving) software running on a machine that does not

produce a paper record, not only has the potential to alter the vote tally but can also make it *impossible* to conduct a meaningful audit or recount (or even to detect that an attack has occurred) after the fact." *Id.* (emphasis added); *see also* Benjamin Bederson, et al., *Electronic Voting System Usability Issues*, *in* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *2–3 (Apr. 2003) (concluding that printed records of votes are a "simple solution" to the problem of vote verification, in the face of either a malicious attack or a technological mishap); Dan S. Wallach, *Security and Reliability of Webb County's ES&S Voting System and the March '06 Primary Election* *8 (May 2, 2006) ("[A] large number of computer science researchers and others have favored the use of paper ballots in conjunction with electronic voting systems" because "[s]uch hybrid systems . . . preserve many of the benefits of paper (notably its permanence and relative immutability) while also having the benefits of computer systems . . . ."), *available at* http://accurate-voting.rice.edu/wp-content/uploads/2006/09/webb-report2.pdf.

For precisely these reasons, experts studying the type of iVotronic DRE system in use in South Carolina have advocated for a "paper trail" to confirm that votes are not altered or inadvertently miscounted. *See* Alec Yasinac, et al., *Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware: Final Report for the Florida Department of State* 35 (Feb. 23,

2007), *available at* https://people.eecs.berkeley.edu/~daw/papers/sarasota07.pdf. The Yasinac study noted that, in addition to the absence of paper confirmations, South Carolina's iVotronic DRE system lacks electronic audit logs that record "all user interactions with the system." *Id.* at 35–36. These missing controls, if implemented, would "significantly enhance [the] ability to perform meaningful election audits after the fact." *Id.* at 35–36. Other studies have similarly identified obstacles to performing reliable audits of voting records in the iVotronic system, including that the system does not record when a terminal is opened by a poll worker or when a terminal is not in use; a pervasive issue of incorrect internal time in terminals; and the existence of event codes for which no explanation aside from the phrase "UNKNOWN" is provided. *See* Duncan A. Buell, *An Analysis of Long Lines in Richland County, South Carolina*, 1 USENIX J. Election Tech. & Sys. 106, 108 (Aug. 2013); Buell & Gay, *Is Technology the Answer?*, at 23.

For all these reasons, the inherent flaws in South Carolina's iVotronic DRE system run deeper than that of over- or under-counting votes. Even when votes are recorded, time and again they have been recorded incorrectly due to calibration or other errors. And, as local election officials recognize, these errors will only get worse as the machines get older. But in the face of these known problems, South Carolina does not even use a reliable election auditing system. That failure allows an unknown number of errors to go undetected and uncorrected. Through its

vulnerabilities and lack of compensating controls, South Carolina's iVotronic DRE system permits the arbitrary abridgement of voters' rights to have their ballots counted for the intended recipient.

C. South Carolina's Voting System Has Known Defects That Make It Susceptible To Manipulation And Attack.

Finally, South Carolina's voting system presents an undue risk of ballot box tampering from wrongdoers here and abroad. State action cannot allow the votes in the ballot box to be intentionally altered. *See Baker*, 369 U.S. at 208.[3] Yet South Carolina has deliberately chosen to deploy a voting system that is uniquely susceptible to manipulation and attack.

This is not the first time that voters have sought judicial intervention to guard their votes against interference. In that regard, courts have recognized that it is not enough for states merely to refrain from stuffing the ballot box. *See Curling*, 334 F. Supp. 3d at 1314–15. Rather, voters may maintain a suit based on allegations that a "DRE voting system was actually accessed or hacked multiple times already – albeit by cybersecurity experts who reported the system's vulnerabilities to state authorities, as opposed to someone with nefarious

[3] In an early case on which the Supreme Court relied for its holding in *Baker*, one of the offenses against the right to vote was "refusing to allow the supervisor of elections to inspect the ballot box, or even to enter the room where the polls were held." *Ex parte Siebold*, 100 U.S. 371, 379 (1879) (cited by *Baker*, 369 U.S. at 208). In other words, an injury to an election's integrity can frustrate the right to vote.

purposes." *Id.* at 1314 (emphasis removed). In such hacking cases, the plaintiffs' injury is "specifically to their fundamental right to participate in an election process that accurately and reliably records their votes and protects the privacy of their votes and personal information." *Id.* at 1315. Put simply, states cannot refuse to "take[] steps to secure the DRE system from such attacks." *Id.* at 1316.

Evidence of cyberattacks on state election systems is not merely speculative; past cyberattacks and the substantial threat of future attacks has been demonstrated through recent legal proceedings against the cyber-attackers. Last July, Special Counsel Robert S. Mueller III issued an indictment against 12 Russian intelligence officers, accusing them of extensive cyberattacks targeting the November 2016 general election that included "attempts to break into state elections boards." Mark Mazzetti & Katie Benner, "12 Russian Agents Indicted in Mueller Investigation," *New York Times* (July 13, 2018), *available at* https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html. The indictment specifically alleged that Russian cyber-attackers "targeted state and county offices responsible for administering the 2016 U.S. elections." *United States v. Netyksho, et al.*, 1:18-cr-00215-ABJ (Indictment ¶ 75) (D.D.C. July 13, 2018).

Earlier this month, a joint intelligence bulletin issued by the Department of Homeland Security and Federal Bureau of Investigation confirmed that these

Russian hacking activities targeted the election systems in all 50 U.S. states. *See* Sean Gallagher, "DHS, FBI Say Election Systems in All 50 States Were Targeted in 2016," *Ars Technica* (Apr. 10, 2019), *available at* https://arstechnica.com/information-technology/2019/04/dhs-fbi-say-election-systems-in-50-states-were-targeted-in-2016. The U.S. law enforcement agencies described these efforts as "methodical reconnaissance" in which the Russian hackers "prob[ed] for potential vulnerabilities in election systems" at "both the state and local level." *Id.* Though the extent of the Russian hackers' efforts in each state have not been publicly disclosed, it is clear that South Carolina's voting system was not spared in the efforts by Russian cyber-attackers to manipulate the 2016 U.S. election.

South Carolina's voting system in particular has already been shown to be vulnerable to hacking. At a recent conference, computer hackers with only legally and publicly available information were able to breach a range of actual voting machines—including the type of ES&S iVotronic DRE machine used in South Carolina. *See* Matt Blaze, et al., *DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure* 4, 8 (Sept. 2017), *available at* https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf. The subsequent report noted that many of these machines include hardware components manufactured outside of the United States, which exposes voting

machines to compromise "at the earliest stages in [the] manufacturing process." *Id.* at 15. "For example, foreign actors could design or plant a virus in software, memory, or even a small microchip that could affect an entire make/model of voting machine, theoretically allowing them to be compromised in one coordinated attack." *Id.*

An earlier study conducted for the State of Ohio found that the ES&S iVotronic DRE and other ES&S systems "lack the fundamental technical controls necessary to guarantee a trustworthy election." *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing: Final Report* 29 (Dec. 7, 2007), *available at* http://gaverifiedvoting.org/pdf/iv-source-documents/2007-Univ-Pennsylvania-EVEREST-Hart.pdf. The researchers identified multiple errors—including unsafe coding practices and the failure to protect data and software with passwords and cryptology—that allow "even persons with limited access . . . to compromise voting machines and precinct results." *Id.* The study concluded that the security vulnerabilities of ES&S systems are "severe and pervasive." *Id.* at 30.

Another report prepared for the State of Florida detected "significant password weaknesses," along with several mechanisms through which a virus could be introduced into the iVotronic DRE system, including "buffer overflow vulnerabilities" and source code problems found in the devices used to collect

votes from terminals. *See* Yasinac, et al., *Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware* at 36–45; *see also* Wallach, *Security and Reliability of Webb County's ES&S Voting System* at *2–8 (identifying multiple security vulnerabilities with the iVotronic DRE system, such as overly simple default passwords; the inability to assess whether firmware run by the machines is "official"; and inadequate protections against tampering with the machines' "flash cards," which store voting data).

The threat of election hacking in South Carolina remains an imminent risk in the future, because the State has failed to take measures to protect the system from hacking despite knowing of these concerns. *See Curling* 334 F. Supp. 3d at 1316. In a recent report on election security in all 50 states, the Center for American Progress gave South Carolina's voting system a grade of a "D," noting that "[t]he state's use of machines that do not provide a paper record and its lack of robust post-election audit leaves South Carolina open to undetected hacking." Danielle Root, et al., *Election Security in All 50 States: Defending America's Election* 159 (Feb. 2018), *available at* https://cdn.americanprogress.org/content/uploads/2018/02/21105338/020118_ElectionSecurity-report11.pdf. South Carolina continues to use the ES&S iVotronic system even after a recent security breach at the company released "encrypted [versions of] passwords for ES&S employee accounts," which could be used by sophisticated attackers "to infiltrate company systems." Frank

Bajak, "US election integrity depends on security-challenged firms," *AP News* (Oct. 29, 2018), *available at* https://www.apnews.com/f6876669cb6b4e4c9850844f8e015b4c. The State's use of ES&S iVotronic DRE machines—a system known to be vulnerable to multiple types of attacks by malicious actors, including through security breaches at ES&S itself—presents a serious risk of ballot box tampering.

CONCLUSION

For the foregoing reasons, the district court's order dismissing Plaintiffs' Complaint should be reversed, and the case should be remanded for further proceedings.

Respectfully submitted,

s/ *Philip S. May*
John D. Graubert
Philip S. May
Megan O'Neill
Adam G. Crews
Jessica Jensen
COVINGTON & BURLING LLP
850 Tenth St. NW
Washington, D.C. 20001
(202) 662-6000
PMay@cov.com

Counsel for Amici Curiae

Ronald Fein
John Bonifaz
FREE SPEECH FOR PEOPLE
1340 Centre St. #209
Newton, MA 02459
(617) 244-0234
RFein@freespeechforpeople.org

April 15, 2019

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitations of Federal Rules of Appellate Procedure 29(a)(5) and 32(a)(7)(B) because it contains 5,008 words, excluding the parts of the brief exempted by the Federal Rule of Appellate Procedure 32(f).

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in Times New Roman 14-point font.

s/ *Philip S. May*
Philip S. May
Counsel for Amici Curiae

April 15, 2019

CERTIFICATE OF SERVICE

I certify that on April 15, 2019, the foregoing document was filed electronically through the Court's CM/ECF system, which caused a true and correct copy to be served on:

Jamila Goldkamp Benkato
Email: jamila.benkato@protectdemocracy.org
2020 Pennsylvania Avenue, NW
Washington, DC 20006

David Stanley Frankel
Email: DFrankel@kramerlevin.com
1177 Avenue of the Americas
New York, NY 10036-0000

Jessica Ann Marsden
Email: jess.marsden@protectdemocracy.org
510 Meadowmont Village Circle
Chapel Hill, NC 27517

Harry Pattridge Morgenthau
Email: hmorgenthau@kramerlevin.com
1177 Avenue of the Americas
New York, NY 10036-0000

Laurence Michael Schwartztol
Email: larry.schwartztol@protectdemocracy.org
125 Walnut Street
Watertown, MA 02138

Thomas Parkin Hunter
Email: phunter@scag.gov
P. O. Box 11549
Columbia, SC 29211-1549

Harley Littleton Kirkland
Email: hkirkland@scag.gov
P. O. Box 11549
Columbia, SC 29211-1549

Wesley Aaron Vorberger
Email: wvorberger@scag.gov
P. O. Box 11549
Columbia, SC 29211-1549

April 15, 2019

s/ *Philip S. May*
Philip S. May
Counsel for Amici Curiae